Olistek N.V. POLICY

for Prevention and Combatting of Money Laundering and Terrorist Financing

VERSION CONTROL

Version	Version Date	Approved By
2.0	29 January 2025	The Board

CONTENTS

VERSION CONTROL 1
CONTENTS 2
ABBREVIATIONS 3
1. PREAMBLE 4
THE POLICY 4
DEFINITION OF ML, TF & FP 4
TARGETED FINANCIAL SANCTIONS 5
PURPOSE OF THE POLICY 5
2. RISK BASED APPROACH 6
DEFINITION 6
BUSINESS, CUSTOMER & SECTOR RISK ASSESSMENT 7
INTERNAL CONTROLS & AUDIT FUNCTION 12
AML&TF DESIGNATED OFFICER 13
3. CUSTOMER DUE DILIGENCE 14
INTRODUCTION 14
THE CDD MEASURES 14
ENHANCED DUE DILLIGENCE 16
SIMPLIFIED DUE DILLIGENCE 17
POLITICALLY EXPOSED PERSONS 17
ESTABLISHMENT OF PURPOSE OF BUSINESS RELATIONSHIP 18
CONFIRMATION OF UBO OF THE FUNDS 18
IDENTIFICATION AND VERIFICATION SYSTEMS 19
4. MONITORING 20
ONGOING MONITORING OF IDENTITY 20
TRANSACTIONS MONITORING 20
MONITORING OF THE ACCOUNT ACTIVITIES 21
MONITORING OF HIGH-RISK CLIENTS 22
REPORTING SUSPICIOUS ACTIVITIES AND TRANSACTIONS 23
5. EMPLOYEES 23
STAFF RELIABILITY AND PROBITY 23
SCREENING 24
PROFESSIONAL SUPPORT AND TRAINING 25
AML TRAINING 25
6. RECORD-KEEPING 26
7. RATIFICATION 27
APPENDICES 28
APPENDIX A. OPERATING CONTROL MATRIX (FRAGMENT) 28
APPENDIX B. SAMPLE OF CUSTOMER TRACK-RECORD 29
APPENDIX C. REPORT ON SUSPICIOUS ACTIVITIES AND TRANSACTIONS 30

ABBREVIATIONS

AML, TF & FP ..... Anti-money laundering, prevention of the terrorist financing & financing of proliferation

BO ..... Beneficial Owner

CDD ..... Customer Due Diligence

CEO ..... Chief Executive Officer

CFATF ..... Caribbean Financial Action Task Force

CFO ..... Chief Financial Officer

CRA ..... Customer Risk Assessment

EDD ..... Enhanced Due Diligence

FATF ..... Financial Action Task Force

FIU ..... Financial Intelligence Unit

KYC ..... Know your customer

MLRO ..... Money Laundering Reporting Officer

NOIS ..... National Ordinance on Identification of clients when Rendering Services

NOPML ..... National Ordinance Penalization of Money Laundering Regulations

NORUT ..... the National Ordinance on the Reporting of Unusual Transactions

NRA ..... National Risk Assessment

PEP ..... Politically Exposed Person

RBA ..... Risk Based Approach

Regulations ..... Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

SDD ..... Simplified Due Diligence

SoF ..... Source of Funds

SoW ..... Source of Wealth

STR ..... Suspicious Transaction Report

The Policy ..... the Policy on Prevention of Money Laundering and Terrorist Financing

UBO ..... Ultimate Beneficial Owner

URT ..... Unusual Transaction Report

1. PREAMBLE

THE POLICY

The Policy outlines the general unified standards and procedures of AML, TF & FP which must be adhered to by Olistek N.V. (Hereinafter — «the Company») its directors, officers and employees.

The NOIS, NORUT, the Sanction National Ordinance, and the Kingdom Sanction Act all contain provisions requiring service providers to take measures to prevent their services from being used for money laundering, terrorism financing, and the proliferation of weapons. Please also refer to the dedicated Olistek N.V. Sanction Policy which comes as an integrated part of the main company's AML policy.

Countries collaborate to combat these issues through the FATF, which was established during the 1989 G-7 Summit in Paris. The Dutch Kingdom is a member of the FATF, while Curaçao is part of the CFATF.

- article 2 paragraph 8 and article 11, paragraph 3, of the NOIS (N.G. 2017 no. 92) and;
- article 22mm, paragraph 3, of the NORUT (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54)

Among others, current AML policy refers to:

- The NOIS (N.G. 2017, no. 92);
- The NORUT (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the NORUT
- (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security
- Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security
- Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions
- Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

DEFINITION OF ML, TF & FP

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three phases.

Cash first enters the financial system at the "placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Broadly, the international AML, TF & FP provisions are aimed at requiring firms to:

- identify customers and suspicious transactions at the placement and layering stages
- keep adequate records which should prevent the integration stage being reached, and also provide an audit trail for investigators, and
- report suspicious activity or behavior to the relevant regulatory or legislative authority.

Terrorist financing may not always involve funds derived from criminal activities; instead, it often seeks to hide the origin or intended use of funds, which could be for illicit purposes. The primary distinction between terrorist financing and money laundering lies in the source of the funds. Unlike traditional criminal organizations, terrorist financiers may rely on legitimate sources of funding. These sources can include charitable donations, foreign government support, business ownership, and personal employment. Despite differing motivations, the methods used to finance terrorism can be similar to those employed by criminals to launder money. Terrorist operations may not require large sums, as funding can be accumulated over time, with transactions that are relatively simple and not immediately suspicious.

FP is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions require countries to freeze funds and assets, ensuring that no funds or assets are made available, directly or indirectly, to designated persons or entities. In Curaçao, all individuals and legal entities must promptly and without prior notice freeze the funds or assets of designated persons and entities. This obligation aligns with United Nations Security Council resolutions and the European Union's Common Foreign and Security Policy. Compliance with UN Security Council sanctions is mandatory under the United Nations Charter, while EU sanctions are binding on Curaçao through the Kingdom Sanctions Act. Mechanisms must be in place to verify the sanction status of withdrawing participants to prevent sanctioned individuals or organizations from accessing funds that should be frozen.

PURPOSE OF THE POLICY

As indicated, the Regulations are applicable for Curaçao Gaming Sector in order to combat ML, TF and FP, and are effective as of 10 April 2025. All online operators are bound to comply with these Regulations in order to ensure that the Company is fully comply with applicable AML, TF & FP and terrorism financing laws and regulations of respective countries and jurisdictions. The Company is committed to annual review and critical reassessment of this Policy in light of the Company’s business strategies, goals and objectives on an ongoing basis.

2. RISK BASED APPROACH

DEFINITION

As any online funds' recipient and processing business, the Company is exposed to a variety of risks related to a potentially improper use of the its business facilities in the interests of those involved in money laundering and terrorist financing. While these risks are inherent and cannot be entirely avoided, the Company believes that the risks could be identified and contained via effective use of the AML&TF procedures, systems and personnel.

The foundation of the risk-based approach is the risk assessment that the Company must conduct on its own operations. This involves understanding and evaluating the general risks to which the business is exposed, known as the business risk assessment.

The Company has identified the following key ML&TF risks.

1. The risk of accepting the customers whose identities and/or addresses are hidden to conceal the direct relation to ML&TF activities (for example, use of multiple passports to conceal the true identity or residential address.)
2. The risk of taking, as a deposit for online gaming via the Company's website, the funds that have, unbeknownst to the Company, been originated from illegal and/or terrorist-supporting sources (for example, transfer of gambling funds directly or indirectly from FATF-censured jurisdictions.)
3. The risk of providing an unintended financial conduit or repository for the funds originated in the course of illegal and /or terrorist-supporting activities (for example, temporary "parking" of funds without the direct use in e-gambling activities.)
4. The risk of the illegal funds transfers (withdrawal) by the customers via Company's website facilities (for example, placing the funds without intention of using them in betting activities).
5. The risk of unknowing conduct, by the Company, of certain functions of a financial institution for any of the customers beyond the usual business remit (for example, by saving, exchanging or transferring the customer funds at the customer requests).

An anti-ML compliance program is an essential component of a Company's compliance regime. The primary goal of every good program is to protect the organization against ML and to ensure that the organization is in full compliance with relevant laws and regulations.

Based on the FATF Recommendations, igaming companies are required to apply a Risk-based Approach to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified.

Applying Risk-based Approach means that the Company:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

Risk assessment process for ML&TF threats is arranged along two different dimensions – nature and complexity of the risk; and value of the risk.

- Along the first dimension, there are a number of risk triggers that allow for identification of the nature and complexity of the risk, i.e., citizenship of the player, changes in the registration information, e-wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the ML&TF risk is simple or complex in nature. Relative simplicity or complexity further determines the Company's response and mitigation measures towards the risk.
- Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific ML&TF risk. For example, the first deposited amount from a new client is usually accepted at the lowest allowable threshold, thus containing the ML&TF risk of improper use of the Company's Customer account for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the values of allowable deposits and withdrawals. Gradually, the Company's relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Given that risks are dynamic, the Company subscribes to continuously monitor the effectiveness of these policies, procedures, and controls, making necessary adjustments as needed. The risk assessment must also be made available to the GCB upon request.

BUSINESS, CUSTOMER & SECTOR RISK ASSESSMENT

The higher the risk, the more measures the Company has to take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower, they may take simplified measures, provided that this is consistent with the country's assessment of its money laundering/financing of terrorism risks. Following risk segments have to be considering during the operation.

BUSINESS RISK ASSESSMENT

The Company carries a business risk assessment to identify the ML/TF risks it is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment addresses the ways in which the products and services could be used to launder money, finance terrorism and finance proliferation and the extent of the risk that this will happen. Special consideration is given to the type of customers, products and services offered, delivery channels and geographical risk factors. The Company includes the outcomes and recommendations of the NRA in its business risk assessment, which allows to set a risk appetite. The effectiveness of the implementation of these measures has to be monitored and improved where necessary.

The Company subscribes to revise the business risk assessment whenever there are changes to the environment, such as introduction of new payment methods, new markets, new games or regulatory changes. In the absence of changes, the Company will assess its business risk at least once a year, to evaluate whether any changes thereto are necessary. In order to work risk-based, it is important that the Company continuously follow the latest reporting regarding money laundering and terrorist financing.

This risk assessment has to be documented, approved by the Board of directors of the Company and made available to the GCB upon request.

All aspects of the Business Risk Assessment should be covered, including:

- The methodology adapted;
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

CUSTOMER RISK ASSESSMENT

Each player presents unique risks to the Company. As a result, a player-specific risk assessment is necessary for the Company to identify potential risks associated with establishing a business relationship or conducting a one-time transaction with a player, referred to as the CRA. This assessment allows the Company to create a risk profile for the customer and categorize the money laundering or terrorist financing (ML/TF) risk posed by the player as low, medium, or high.

The customer specific risk assessment is carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. The initial customer specific risk assessment can be revised at a later stage of the business relationship, which might result in customer's risk rating adjustment.

There are a number risk triggers that allow for identification of the nature and complexity of the risk, i.e., citizenship of the player, changes in the registration information, e-wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the ML&TF risk is simple or complex in nature. Relative simplicity or complexity further determines the Company response and mitigation measures towards the risk.

Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific ML&TF risk. For example, the first deposited amount from a new customer is usually accepted at the lowest allowable threshold for a given jurisdiction thus containing the ML&TF risk of improper use of the Company's Client account facilities for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the values of allowable deposits and withdrawals. Gradually, the Company's relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Based on the dimensions described above, a specific ML&TF risk is classified as low, medium and high; depending on classification, different actions are called for from the MLRO and other employees involved in ML&TF controls. Typical actions for high-risk detection situations are increase in the time lag for withdrawals and acceptance of the customer funds and enhanced verification of the customer.

On the basis of the CRA, the proper level of CDD is applied. All the measures stated above are documented and approved by the Board of directors.

SECTOR RELATED RISK ASSESSMENT

The Company operation covers a vast set of countries, some of which might possess strategic deficiencies as per FATF. Such characteristics impose the requirement for the Company to be alerted in its approach towards various risks of regional nature that might impact the Company's business.

This means that the Company employs a policy of high alertness when entering a new market, managing its current operating exposure strictly conditional upon the proven market potential and the acceptable levels of legislative recognition conducive to the Company's business in a given country. By necessity, thus the conduct of general business risk assessment is country-based and country specific in nature.

There are four sector related risk areas that the business has to cover, as follows:

1. Customer risk

It arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or SoW. Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;

- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple accounts to hinder Company's tracking of their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (monitor player activity and issues and collect credit).

The Company must set a value which represents the upper value of a typical player's transactions. A player having a single source of regular income will pose a lesser risk of ML/TF than a player who has multiple sources of income or irregular income streams.

2. Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the player and the SoW of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk. A variety of sources is accounted when searching for information produced by the FATF and non-governmental well-known bodies. Some sources to use are:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The Company has a list of countries that are considered as high risk and those that are considered low risk.

3. Product, service and transaction risk.

Specific payment methods, which are considered to present a higher risk of ML/FT, are treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of gaming accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g., roulette, craps → even bets);
- The use by customer of accounts held or cards issued in the name of third parties;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Multiple accounts or wallets (the Company may own and control multiple web sites);
- Changes to financial institution accounts to fund player's account;

- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;

- Using cash to fund a pre-paid card poses similar risks as cash;

- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Company. This may be useful for dishonest customers who wish to disguise their gambling.

4. Distribution channels risk

The channels through which the Company establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:

- Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;

- While situations where interaction with the customer takes place on a non-face-to-face basis no longer led to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high-risk factor for risk assessment purposes unless the Company adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;

- Where there is the involvement of a third party in the interactions between the customer and the Company, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

OTHER RISKS

The Company will also take into account some risk hypotheses / indications which may lead to the recognition of suspicious, complex or unusual transactions or other risks:

1. Potential complicity of employees;
2. Use of false or stolen identity documents by players;
3. Concealment of the identity of the BO;
4. Lack of appropriate KYC policies;
5. Accessing multiple gaming platforms or collections of games within the same platform;
6. Complicity in the provision of bonuses or other benefits;
7. B2C; the vulnerability is associated with the ability of clients to join the game and deliberately transfer funds ("chip dumping");
8. E-Wallet, being considered a payment method that makes difficult for the Company to identify the SoF;
9. Remote gambling used as a front for cash deposits, which are then transferred to bank accounts, with apparent winnings from gambling as the SoF;
10. Transactions, both individual and linked, that are unusual in character, complex, large and have no obvious economic, commercial or legal purpose in relation to the Company's business;
11. Transactions that present an unusual or complex pattern compared to the client's risk profile or the pattern of transactions associated with the client, similar products or services;
12. Transactions in excess of normal limits typical for a player. An example would be an attempt to withdraw the funds from the gaming account in small instalments but totaling the entire balance of the account during a short period of time;
13. High turnover financial transactions (deposits and withdrawals) unwarranted by the gaming activity of the player;
14. Transactions outside of the player's regular payment and withdrawal patterns. An example is a series of minor deposits followed by no-activity period and a subsequent request for withdrawal of the entire amount;

15. The customer requests unnecessary or unreasonable levels of secrecy. For example, the client is reluctant to share due diligent information, or he appears to want to disguise the true nature of his business;
16. If the customer's or BO's SoW or SoF cannot be easily explained;
17. Transactions of the customer, who has a political connection, or any other relevant links to a PEP or a Family member of PEP or Persons known to be close associate of PEP (persons who may abuse, directly or indirectly, of a public position for private gain), if such connection/link becomes known to the Company;
18. The customer insists that the transfer of earnings be made to the account or in the name of another person;
19. Customers who constantly play against each other;
20. Clients who carry out transactions that appear to be disproportionate compared to the financial situation or income proven according to the documents certifying the source of the funds.

The Company recognizes that in addition to the indications of risks listed above there may exist various other unforeseen ML&TF risks. While prior identification of all such risks is not possible, the Company believes that fostering the general alertness, risk awareness and the spirit of constructive skepticism among employees are the best general preventive measures that could help timely identification recognition of suspicious transactions in terms of ML&TF risks. The management believe that fostering the general alertness, risk awareness and the spirit of constructive skepticism among employees is the best general preventive measure that could prevent ML&TF risks from materializing.

In general terms, the Company will examine the context and purpose of all transactions that meet at least one of the following conditions:

a) are complex transactions;
b) are transactions with unusually high values;
c) do not fit into the usual pattern (taking into account any reasonable or justified deviations from the pattern);
d) do not have an obvious economic, commercial, or legal purpose.

In any of these cases, the Company will increase the degree and nature of the monitoring of the Business Relationship in order to determine whether such transactions or activities are suspicious.

The identification of an isolated risk factor does not automatically determine the classification of a client in different risk categories. For each client, the Company will evaluate the risk factors to establish the degree of risk, which will be established as a result of the logical combination of the identified risk factors. The placement of a client in one of the risk categories can be changed at any time during the Business Relationship as a result of obtaining new information.

TEHCNOLOGICAL DEVELOPMENTS RISK ASSESSMENT

The Company has appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It monitors and assess the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

A risk assessment takes place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism.

INTERNAL CONTROLS & AUDIT FUNCTION

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business and provision of the safe and fair gambling environment for the customers. Overall logic of the internal controls at the Company is described by Operating Control Matrix (presented in Appendix A). The Matrix is a practical guidance on various controls mandatory for execution in the course of the daily business of the Company. The matrix is updated on an annual basis to reflect the changing business requirements and regulatory changes in the markets in which the Company operates.

The AML compliance program is monitored and evaluated at least annually by an outside independent party based on an outsourcing agreement. The people performing the audit are in no way involved with the Company's AML compliance staff and are sufficiently qualified to ensure reliability of the delivered results. The audit covers information including:

- An evaluation of the Company's AML & CTF policy;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The assessment will also include an analysis of whether the Company was responsive to earlier audit findings. All the results are documented with the deficiencies reported to the designated MLRO officer, with a request to take prompt corrective actions by a certain deadline.

AML&TF DESIGNATED OFFICER

MLRO has working knowledge of the Company business environment, risks inherent to the Company's business model and AML&TF provisions as stipulated in the Regulations as amended. AML&TF Compliance Officer also performs the duties of MLRO at the Company and is responsible for reporting transactions suspicious from AML&TF standpoint to FIU Curacao.

General duties of the AML&TF Compliance Officer include monitoring of the Company's compliance with the AML&TF obligations, assessment of the business risks both internal and external, oversight of the AML&TF related communication and training for employees, and reporting of the findings and critical issues of the AML&TF systems and procedures to the managers and executives of the Company. The AML&TF Compliance Monitoring Officer/MLRO ensures that the Company keeps and maintains all required AML&TF records and that Suspicious Activity Reports are filed with FIU Curacao when required and appropriate.

The AML&TF Compliance Officer is vested with full responsibility and authority to enforce the Company's AML&TF Policy and working procedures. Responsibilities of AML&TF Compliance Officer includes:

- Spearheads the global AML&TF drive and is responsible for the overall AML&TF strategy and policies of the Company.
- Conducts escalation and sanctioning in cases of internal non-compliance or lack of quality with AML&TF strategy and policies.
- Represents AML&TF activities at the senior management level.
- Manages central AML&TF function and controls adequacy of policies, organizational structure and resources devoted to AML&TF compliance.
- Drives communication to the senior management and other stakeholders with respect to issues concerning AML&TF compliance.
- Maintains relationships between AML&TF function and external auditors, regulators and other compliance authorities.
- Oversees and presents to the senior management overview and budget of the AML&TF activities on a yearly basis.
- Contributes to the elements of the IT-systems related to AML&TF compliance.
- Presents to senior management the yearly AML&TF Compliance Report.
- Reports to senior management all cases of non-compliance or inadequate compliance with AML&TF policies and procedures on ongoing basis, together with recommendations for improvement.

3. CUSTOMER DUE DILIGENCE

INTRODUCTION

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. It must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions. A sound CDD program is the best way to prevent AML, TF & FP.

The customer's risk profile is essential to apply a certain level of CDD commensurate to the identified ML/TF risk. The purpose of collecting information is to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior, which are reported to the FIU (more on chapter 4).

The obligation to undertake CDD measures when:

- When players engage in financial transactions equal to or above EUR 2,000;
- carrying out occasional transactions above the monetary equivalent of EUR 2,000;
- there is a suspicion of money laundering or terrorist financing; or
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of EUR 2,000.

For transaction above the monetary equivalent of EUR 2,000, CDD measures are applied immediately. Whether the transaction is carried out in a single operation or in several operations which appear to be linked. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. A transaction consists of the wagering of a stake or the collection of winnings.

The main responsible department for the Due Diligence process is Factoring and Monitoring (Anti-fraud) Department. In order to perform the due diligence controls, employees use automatic controls, manual reviews and electronic registers.

THE CDD MEASURES

The CDD measures are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the BO, and taking reasonable measures to verify the identity of the BO, such that the Company is satisfied that it knows who the BO is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the player, its business and risk profile, including, where necessary, the SoF.

The Company, its directors, officers and employees are prohibited to disclose the fact that an UTR is being reported to the FIU. A risk exists that players could be unintentionally tipped off when the Company is seeking to perform its CDD obligations in these circumstances. Therefore, if the suspicion arises those transactions relate to ML or TF, the risk of tipping-off should be accounted when performing the CDD process. If there are reasonably believes that performing the CDD process will tip-off the player, there is the option of not to pursue the process and file an UTR to the FIU.

IDENTIFICATION AND VERIFICATION OF THE PLAYER

Identification and verification of the player refers to the collection of personal details of the player to establish the identity of the player. Verification on the other hand consists in confirming the personal details collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk.

When identifying the player, at a minimum the following information is collected:

- full name;
- permanent residential address;
- date of birth;
- place of birth;
- nationality; and
- identity number.

However, in low-risk scenarios identification can be limited to full name, permanent residential address and date of birth. On the other hand, in high-risk situations, additional personal can be collected as necessary to mitigate the higher risk of ML/FT.

CRA is done to have sufficient information available to detect unusual activity in the course of the business relationship. A provisional risk rating is assigned based on the initially collected information and is revised once questions are answered or additional information received. On the basis of the CRA, the proper level of CDD can be applied as stipulated by the CAP.

Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

Verification of identity is carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g., passport, identity card). Where such a document does not allow verification of the player's residential address, other documents are requested, like a bank statement, utility bill[1], letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. The client can be contacted by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies' registries or media and news sources. Biometric checks can also be used to confirm that the individual providing the document is the one described therein. The Company also cross references the information with geo-location information, IP address data, funding method data etc.

Verification is carried out to determine that the player is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. Extra care is taken with regard to verifying the authenticity of foreign documentation, particularly where the type of document is unfamiliar.

When there is not sufficient comfort that the Company knows its player, it is expected that additional measures are to be taken. Some of these measures include requesting additional identification documents, asking the player

[1] For phone bills, only fixed line telephone bills are accepted as proof of address.

to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

TIMING OF CDD MEASURES

Verification of identity is conducted when engaging in financial transactions equal to or in excess of EUR 2,000. However, a minimum level of CDD measures is required prior to reaching the threshold. Thus, simultaneously with the opening of an account, the customer is identified by collecting the minimum personal details. The threshold is calculated on a daily considering all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers.

In carrying out the CDD measures, customers are allowed to continue using their gaming account while the Company obtains any necessary information from the customer concerned. However, if the EUR 2,000 threshold is reached because of a deposit of the player, he cannot further deposit funds into the account or withdraw funds from the account. He still will be able to play, using the funds already in his account. However, if the EUR 2,000 threshold is reached because the customer wants to withdraw his money, a complete freezing of the account will occur and the customer would not be able to play.

Besides that, if the requested information and documentation is not received within 30 days from the moment the EUR 2,000 threshold was reached, the Company will terminate the relationship with the player and its MLRO will report the transaction to the FIU, only if a presumption of ML & TF exists*. If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.*

If no presumption of ML & TF, the funds will be transferred to the same bank account or wallet it was deposited from.

ENHANCED DUE DILLIGENCE

Whenever an occasional transaction presents a high risk of ML/TF, the EDD measures must be applied. Enhanced Customer verification could be done in any time of the customers' activity, starting from registration process and continuing through all further processes – deposits, bets, withdrawals.

EDD measures should be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. EDD has to be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher risk geographic areas;
- PEP's;
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the SoF or SoW of the player. Examples of SoF include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;

- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In situations presenting a higher risk of ML/TF, SoF information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

SIMPLIFIED DUE DILLIGENCE

Where the risks of money laundering or terrorist financing are lower, the Company can conduct SDD, which should take into account the nature of the lower risk. Examples of possible measures:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the Company to obtain the player's identity. In this case the Company may limit identification to the first three personal.
- Verifying the identity of the customer and the BO after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g., birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

SDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

POLITICALLY EXPOSED PERSONS

All players are screened against sanctions lists of the UN and EU.

With respect to transactions or business relationships with PEPs, in addition to the KYC measures:

- the Company has in place appropriate risk management systems to determine whether the customer is a PEP;
- apply the following measures in cases of setting relationships with PEPs:
- obtain senior management approval for establishing or continuing business relationships with such persons; - take adequate measures to establish the SoW and SoF that are involved in business relationships or transactions with such persons;
- conduct enhanced, ongoing monitoring of those business relationships.

Before establishing of a business relationship or executing an occasional transaction with a PEP, Anti-fraud department requests adequate documentation to ascertain not only the identity of PEP but also to assess his business reputation (e.g., reference letters from third parties). In addition, the Company will screen against Curaçao's local list of designated persons and organizations, once and if this list will be published by the authority.

The screening is being conducted with the assistance of the third-party KYC solution provider. The solution checks published lists of known or suspected terrorists or other sanctioned persons or companies, mainly:

- UN Sanctions List;
- EU Sanctions List;
- Persons List Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists | Office of Foreign Assets Control;
- Other related lists

ESTABLISHMENT OF PURPOSE OF BUSINESS RELATIONSHIP

The business relationship between the Company and the client is a commercial relationship arising out of the licensed activities of the Company, in which the client is involved. The business relationship between the client and the Company is likely to be contracted when the client registers on the website.

At the inception of the business relationship, the Company take into account the following:

- the risk profile of the customer
- the appropriate CDD measures
- whether it is known or suspected that the customer might legalize revenue from illegal activities

Every customer request for establishment of business relationship is screened against blacklists and verified for the unusual features that might point to an intended abuse of the Company's systems and business practices for AML&TF. The Company only accepts individuals whose personal data, disposition and further behavior patterns specifically indicate intention to lawfully and fairly use Company's betting services. Such intention could be verified only in part at the inception stage of the business relationship hence further controls are implemented as the relationship progresses.

The Company collects, if necessary, information and documentation to establish a customer's SoW as well as the expected level of activity. SoW consists of determining the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. As to the extent of the information that the Company collects, it is essential that this reflects the level of ML/FT risk identified through the CRA.

Where the risk is not high, a declaration from the customer with some details (e.g., nature of employment/business, usual annual salary etc.) is sufficient. Social media can also be used as a source of information.

However, where the risk of ML/FT is higher or there are doubts as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation. In developing a customer risk profile, the Company may also consider using statistical data to develop behavioral models against which to eventually gauge a customer's activity rather than collect SoW information. Where the Company opts to adopt this approach, it can use data collected from the Central Statistics Department such as average national income, average disposable income etc. These indicators should allow the Company to determine the average wagering power of players from a given jurisdiction.

The Company can also use data collected over time to create the profile of an average player. The Company is using this only if the customer-base is wide enough to allow the creation of an average profile. For a limited customer-base, the data is obtained from other players with a similar business model. The use of statistical data is incompatible with high-risk situations as the transactional pattern will fall outside the average behavioral model. In such circumstances, the Company will use SoW information.

CONFIRMATION OF UBO OF THE FUNDS

The ultimate purpose of procedures for monitoring AML-TF compliance is to prevent the operation, under the guise of ordinary players and on the Company's platform, of the individuals related to or involved in money

laundering and terrorist funding activities. Establishment of the identity of the UBO of the funds is thus the key purpose of the AML-TF controls at the Company. Operating Control Matrix sets up a number of barriers to prevent the suspect individuals from access to the Company's legitimate services: credit card verification; denial of service to the customers using someone else's credit cards; single-currency settlement; withdrawal identity verification and many others. There are also delegated responsibilities – for example, for the e-wallets originated deposits, responsibility for customer verification and funds provenance lies with e-wallet.

The Company is required to identify and verify the identity of the BO by making sure that customers are registering an account to play and transact on their behalf. This is mentioned on the website's terms and conditions that a registering player must explicitly accept, together with a declaration on the registration page. The Company will not merely rely on said declaration and will monitor for possible instances where the player is actually playing on behalf of third parties.

IDENTIFICATION AND VERIFICATION SYSTEMS

The Company's identification and verification systems are predominantly computer-based and include various data-bases and cross-checking software. The products of third-party providers, credit-card databases and other sources are utilized in order to control the customer identification and fund-origination risks. The Company's accounting system traces the account movements by individual IP address of the players. List of IP addresses is stored and can be viewed for each game account; all IP addresses are also stored in the logs of the program (including archived). The system has a viewing facility for analysis of a list of players and the number of movements at the specified IP address. Recording of IP addresses allows to track down fraudsters whose activities are connected with gaining access to other customers' player account or gaining possession of their funds.

Operating Control Matrix (Appendix B) describes in more details the key procedures applied at the Company to safeguard the integrity of the customer background checks and to arrange for proper customer identification. In some cases, such as country of residency, age and single-account tests, the controls are automatic (no human involvement). In other cases, e.g., funds ownership and changes in customer information, the Company's officers are personally involved and are required to make professional judgments. The combination of automatic and human-driven controls is a key operating feature of the KYC controls in the Company.

Embargo requirements for ML&TF controls specifically concern two country groups:

- the US List of State Sponsors of Terrorism[2]. Currently the list includes Cuba, Iran, Sudan and Syria.
- the countries and territories with prohibitive and internationally promulgated territorial gambling regulations. Currently the list includes the USA and its dependencies, Israel, France, UK and outlying territories, Italy, Spain, Denmark, the Netherlands and Estonia.

Requests from potential customers from the aforementioned countries and territories (residential addresses and IP addresses) are denied. Furthermore, the names of such customers are retained on record, blacklisted and are routinely screened in any future customer requests. The mechanisms, practices and measures of CDD is outlined in a separate document describing the KYC procedures.

[2] http://www.state.gov/j/ct/rls/crt/2012/209985.htm

4. MONITORING

ONGOING MONITORING OF IDENTITY

In conducting ongoing due diligence on the business relationship, the Company holds accurate and up to date identification data of its customers. Since identity may change due to circumstances, the information must be detected and re-evidenced. The Company requests evidence of identity periodically to detect any changes, refresh the data on key events (i.e., change of payment instrument) or tracks expiry dates on evidence of identity and refreshing it as it expires. The Company determines on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

TRANSACTIONS MONITORING

Monitoring of monetary transactions is a constituent part of the monitoring of the account activities and is described in detail in the Operating Control Matrix. Main purpose of transaction monitoring with respect to ML&TF threats is to identify and to prevent the suspicious transactions from taking place at the business facilities. Various safeguards and awareness triggers are employed in transactions monitoring e.g., absolute monetary limits; single-player-single-account, single-session and single-currency rules; obscure event bets (described in Operating Control Matrix).

Assignment of status (and color grades for visual recognition) to the players according to the types of games and gaming behavior:

- No status: players who have not triggered suspicions with any departments of the Company. Usually applied to new customers, which have not finished verification procedure yet. Limits could be set according to a governmental database of self-limited individuals from specific countries.
- Monitored: players who have gone through full verification (provided the passport data, etc.). The gaming activity of customers in this group was analyzed by the Anti-Fraud Department employees, no suspicious actions were detected at the moment.
- Arbitrage: players with the history of placing sure bets
- Scammers
- Foreigners: players whose country of residence is outside of the Company's core region of operations.
- Suspicious: gaming accounts placed under close monitoring by Payment and Factoring & Monitoring Departments
- Potential VIP players
- Existing VIP players. A group of players, which constantly place bets with amounts over 100 EUR or equivalent in other currencies. Their gaming activity is not limited and they have higher priority in processing transactions.

if the player has a "good" category, it doesn't mean that he drops out of control. Payment and Factoring & Monitoring Departments carry out continuous monitoring of all players and transactions. Employees of the Company seeks to identify the following indications of the potential ML&TF threats:

- Individual or linked transactions which are complex or unusually large with no apparent or lawful economic purpose, including those relative to a relationship;
- Unusual patterns of transactions with no apparent economic or lawful purpose, including those relative to a relationship;
- Transactions which exceed certain limits with no apparent economic or lawful purpose, including those relative to a relationship;
- Very high account turnover inconsistent with the balance;
- Transactions which are outside of the customer's regular transaction activity.

Changes in registered players' information are monitored by Anti-Fraud Department; consistency and significance of changes are analyzed daily; game session patterns are matched against the historic average profile (its IP addresses, his types of games and style of bets, Payment Systems that he uses etc.) for a given game to ensure that, in each particular moment, they resemble the historic gambling trends for the customer. Significant deviations during game sessions are documented, analyzed and reported.

If any unusual behavior is identified by the employees of the Department, they make short time block of the activity on the customer's account in order to check whether the customer performs actions by himself and make investigation on player's activity. As for the internal controls, Anti-fraud department on a daily basis generate Manual adjustment report and review any manual changes that were done to the client's account.

Transaction monitoring is executed to prevent involvement of the Company with ML/TF and to safeguard the reputation of the Company. While in conducting ongoing scrutiny of transactions there are transactions that are not consistent with what it is expected from the customer, the Company establishes the source of the funds used for that transaction. The Company must obtain sufficient information and documentation with regard to the transaction to determine the reason for this deviation. If needed, the risk profile of the customer may have to be revised. After receiving this information, the Company decides whether the transaction is an unusual and needs to be reported to the FIU.

The level of on-going monitoring depends on the risk profile of the customer, but even in low-risk situations there is a degree of oversight to ensure that the business relationship is still considered as a low risk one.

The Company conducts ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Company's knowledge of the customer, the customer's business and risk profile.

MONITORING OF THE ACCOUNT ACTIVITIES

This component is central to the Company's AML&TF efforts. Account monitoring is conducted on the ongoing basis by the officers responsible for various operating aspects of the business. The deposit and withdrawal policies are enforced personally by CFO and MLRO. This enforcement is conducted daily and supported by various thresholds set up to flag the potential problems. Operating Control Matrix describes the controlling processes in detail (Appendix A).

Overall, monitoring of account activities consists of:

- Monitoring of new registrations
- Monitoring of deposit activity
- Monitoring of gambling activity
- Monitoring of account access
- Monitoring of account detail changes
- Monitoring of withdrawal activity
- Monitoring of registration data to ensure it is kept up to date

Critical controlling measures with respect to ML&TF prevention are:

- denial of withdrawals for the inactive funds
- detection of the unusual payment patterns (i.e., deposit activity does not match the betting activity or large deposit movements unwarranted by the betting patterns)
- periodic screening of e-wallets used by the players
- pro-active recognition and prevention of players' fraudulent intentions or activities. This component is an indirect indication of probable ML&TF threats.

MONITORING OF HIGH-RISK CLIENTS

Suspicious players and scammers have the highest risk range of all players. There are several categories of such kind of players and the measures for their detection:

“Review”- this group includes players whose gaming activity is unusual. These accounts are limited by 5-10 EUR or its equivalent in other currencies bet amount or even blocked-in order to prevent fraud. For the “Review” the account will be unblocked only when Anti-fraud or Payment or other departments who detected the trigger would confirm that the customer has passed all the required procedure.

“Betting arbitrage’’ - is an example of arbitrage arising on betting markets due to either bookmakers' differing opinions on event outcomes or errors. When conditions allow, by placing one bet per each outcome with different betting companies, the bettor can make a profit regardless of the outcome. Mathematically, arbitrage occurs when there are a set of odds, which represent all mutually exclusive outcomes that cover all state space possibilities (i.e., all outcomes) of an event, whose implied probabilities add up to less than 1.

‘’Bonus hunting (also known as bonus bagging)’’ is a type of advantage gambling where turning a profit from sportsbook bonus situations is mathematically possible.

“Late Betting”- players that place bets on the matches, which are finished already, but not included to the system, result. Also are detected by gaming patterns, by analyzing time of bets and real time of events happened. Depending on player’s average bet amount the 1-20 EUR or its equivalent in other currencies limit in equivalent could be implemented.

‘’SFM (Suspicion Fixed Matches)’’ when player that often bets on events or leagues that are considered highly corrupt and with a high risk of negotiated matches.

“PEP” - Means a natural person who is or who has been entrusted with a prominent public function in the Republic or another country, a close family member of that persons as well as a person known to be a closely associated with such person. Transactions of PEPs continuously monitored, especially to ensure that the threshold has not been exceeded and that the amounts played correlate with the income profile of the PEP received during the EDD procedure.

Adverse media publications, publicly available registers etc.

Payment systems database – reconciliation to the records of the customers. Anti-fraud and Payment departments often refer to the data provided by the Payment systems in order to reconcile information provided by the customer in his registration form with the information recorded in Payment System database. In the black-lists employees who perform controls can find list of persons, which were blocked according to the certain reasons.

And finally, Payment Systems send automatic or manual notifications, if they detect any suspicious transaction. All these notifications are checked and assessed by the Responsible employees.

After suspending the account, a notification appears on the customer’s page and the Support Team requires information and/or documents in order to check the suspicious action. Also, additional information may be requested from affiliated who are processing deposits and withdrawals from the gaming accounts, in order to obtain information about the origin of the funds.

The customer still has the possibility to enter his personal account during the investigation process but the funds will remain frozen and all transactions blocked until the investigation is completed.

All the investigation steps recorded in the system. If it completed successfully, the responsible employee will unblock the account and the customer can manage his funds again. If there were no response to the notification or the customer provides not enough data to complete the investigation - the account will remain blocked until the requested documents received.

"Problematic Gamblers"- we characterize the players whose behavior is excessive and/or aggressive and in general problematic like harassing the support team staff or whose actions could be classified as compulsive gambling. There are 3 ways of identifying players who display problematic gambling behavior and the respective following steps for each type of it:

I. The customer informs the Support team by himself about his gambling problem through e-mail or chat or telephone. The request can include limits of bets that should be set to the customer OR temporary blocking of the account. After the Anti-fraud department execute the request, the customer notified about the changes done to his account via e-mail.
II. Mathematical review. One of the triggers that monitored by the department is the problematic gambling trigger. It includes the following algorithms: if a gamer has losses, which were increased 10 times during a period of more than 3 months (90 days) the gamer is identified as a problematic one OR if a gamer doubled his losses each month during the last 12 months he is identified as a problematic gambling customer. According to these analyses, the Support department initiates the communication with the customer, where they describe the situation, give links to gambling addiction help websites and propose measures to the customer like self-limitation with the most comfortable and suitable conditions.
III. Support team review. While communicating with the customers, the Support department identifies the problem gambling customers if their chats or calls are harassing to the Support team or other customers or compulsive gambling. One of the main triggers of the compulsive gambling is the constant request of the credit to be issued by the website. (no one can issue any credits to customers).

REPORTING SUSPICIOUS ACTIVITIES AND TRANSACTIONS

All suspicious activities and transactions are recognized and recorded in the system. All suspicious activities / transactions, including attempted transactions reported internally first. Concurrent analysis is conducted on each such activity or transaction in accordance with the Operating Control Matrix. The officers responsible for respective areas of transaction monitoring report the suspicious activities to MLRO immediately upon identification, together with a brief description of specific mitigating measures taken. Such reporting is performed in both oral and written form depending on gravity of an incident reported.

The Company's general approach is to file the written report only in cases of reasonable suspicion of substantial violation of Regulations or substantial threat to the business. A degree to which a particular violation or threat is deemed "substantial" is left to the discretion of the officer in charge of specific controlling area and their respective upper management. Due to the fast-moving nature of the business, the management feels that this approach is fully justified.

Employees' may report a suspected instance of ML/FT to the MLRO even when their immediate superior is in disagreement with them. The MLRO must determine if the information available can be considered as sufficient for STR to be made to the FIU.

The format of the report on suspicious activities and transactions is provided in Appendix C.

5. EMPLOYEES

STAFF RELIABILITY AND PROBITY

The Company represents an amalgamation of appropriately qualified people and past-paced technological innovation. Employees are one of the most valuable assets and a critical component of the Company's operating model. In an intense, gain-driven betting environment, staff reliability and probity are of paramount importance to an extent unseen in other businesses.

The Management of the Company recognizes this and, therefore, the employees are expected to:

- conduct their activities in accordance with direct instructions of the immediate supervisors
- exercise sound judgment in situations requiring initiative and unsupervised decision-making
- behave ethically towards the Company, colleagues, clients and third parties
- be fair, honest, dependable and accountable in business dealings
- avoid business and personal actions that might cast appearance of impropriety or ethical ambiguity
- comply with the respective HR policies and regulatory requirements
- declare any actual or perceived conflicts of interest as soon as such conflicts become known
- maintain confidentiality and prevent the disclosure of the confidential information
- refrain from accepting inducements, incentives, gifts or other benefits from the colleagues and third parties that may lead to, or may be seen as leading to, an unfair advantage to third parties or to unfair treatment of the business
- communicate internally and with the third parties using clear and concise meanings, in a timely manner and via the established communication channels
- decline invitations from the mass media and the Internet-based platforms (forums, info-aggregators, news originators and others) to discuss the Company's business.

SCREENING

The Company developed and supports the HR and control policies and procedures for effective initial screening of candidates and subsequent dealings with employees:

- All personnel undergo the initial procedure for personal identification.
- During the first interview, all candidates are required to complete the ID profile designed by HR Department. The ID profile includes a number of psychological tests designed to determine whether a candidate might inflict, under certain conditions, harm to the Company.
- Upon completion of the ID profile and analysis by the HR Department, the recruiter conducts initial interviews with the candidates using a number of further psychological tests.
- Following the conclusion of the initial interview, the second interview by HR Director is conducted for the successful candidate.
- The next step in the hiring process is a conversation with the subject area manager, followed by the meeting with a member of the internal security department.
- Conduct, by a member of internal security department, of the background check on the candidate including, but not limited to, communication with the previous immediate supervisor of the job candidate; verification of the criminal record; examination of job references and communication with the sources; search in the open public sources and the Internet.

Having succeeded in the screening process in its entirety, the new employees are given the mandatory introductory course in their respective areas for three weeks and have to pass the exams as follows.

Stage 1: Employee adaptation and lectures on the bookmaking basics. Exam.

Stage 2: Lectures on the payment systems. Exam and issuance of the internal certificate.

Stage 3: Learning how to work with the software. Exam.

Stage 4: Lectures on dealing with customer complaints.

Stage 5: Training at the workplace and a final exam.

After successful completion of all five stages, the employee commences the duties in probation mode under close supervision of a member of the internal security department and the direct area manager.

For the candidates applying to executive positions, the hiring procedure involves a mandatory personal conversation with the CEO upon which the final decision to hire is made.

PROFESSIONAL SUPPORT AND TRAINING

The Company supports professional efforts by its employees to remain at the forefront of the best practice and technological innovation in the e-gambling and betting industries. It is recognized that such support may take several forms including but not limited to the on-site and distance training, ad-hoc working groups, technical and situational seminars and some others.

The Company offers training courses and conducts a series of seminars for the employees in the varied subject areas of direct interest to the business.

Trainings in Business Administration are conducted for managers of the Company, which include five main blocks: building of the management platform, forming the levers of managerial effectiveness, integration of the management skills, the development of business in the global sphere, and also training courses of business English are conducted for all employees of the Company.

Professional upgrade courses are conducted internally for the staff of Trading and Operational Departments by the divisional heads and Directors of respective departments.

Marketing Department staff participates in various training conferences on various aspects of marketing, including the practice of e-mail marketing; SEO optimization, ICE Totally Gaming, web analytics, etc.

The Finance Department staff participate in training courses on the subjects of management accounting, budgeting and planning, internal controls, and management finance.

AML TRAINING

The MLRO is responsible for the conduct of the introductory AML&TF training course for every new employee and the subsequent AML&TF updates in the "what?" and "how to?" format including:

- what is the employee role in the Company's compliance effort and how to perform the individual compliance duties?
- what are and how to identify red flags and indications of money laundering that may arise in the course of the employee daily duties
- what to do once the risk is identified (including how, when and to whom to communicate the initial suspicion and how to escalate the level of awareness of the threat for further processing and analysis) - what are the latest tools, updates and improvements in the AML&TF investigations.

The MLRO keep a register of all trained employees of the Company dealing with monitoring of transactions, engaged in the management of the Company, any authorized representatives and/or responsible persons.

6. RECORD-KEEPING

The Company is keeping, for at least five years, all necessary records on transactions (both domestic and international), to comply with information requests from the competent authorities. These records permit reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity. From the collected information, the following is being kept:

1. A complete history of each player's account transactions starting from the date of account opening and to his latest bet is saved on the computer system. The system keeps the following information (Appendix B contains a sample of the customer account history):
2. Primary customer data (required at the registration stage) and scanned documents. The fullness of the data required in each particular case is driven by the risk triggers described in Section 3 of this policy i.e., country of the player, currency selected, e-wallets used and other. If a combination of risk triggers gives rise to a particular concern, the employees of Anti-Fraud Department and Payment and Anti-Fraud Department react according to the set of given circumstances.
3. Comments by the employees of the respective departments concerning each player account. There are fields designated to comments in the program for four departments: Anti-fraud, Payments, VIP Players and Support. Each department provides comments (notes) in their respective fields only and strictly in accordance with their official duties. For example, the VIP Players Department usually provides ranking information of VIP players (ranked by stars: from a "small" VIP player to the largest according to graduation, etc.).

When the comments lose relevance with the passage of time, head of the appropriate department may remove a comment however the log will be kept on record indefinitely.

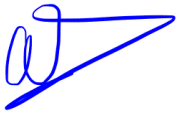
4. System also keeps records regarding profitability of each gaming account for the entire period of its existence – also utilized as an ML&TF risk trigger.
5. All suspicious activities and transactions are recognized and recorded in the system. Concurrent analysis is conducted on each such activity or transaction in accordance with the Operating Control Matrix. Upon receipt of the Report on suspicious activities and transactions, MLRO decides as to the further course of actions concerning possible reporting of the transactions to authorities and licensing authority.
6. All transactions history of a player including amendments, additions and deletions to the transactions are kept for records for 5 years' period. For CDD data and information, the holding period is 5 years following the date of cancellation of customer relationships. Records are maintained on company servers and instantaneous back-up is performed.
7. The system provides technical facilities for sending the messages to clients; such messages are stored in a special Message Box in the context of each player account, as well as in the logs of the system. Disputes with the player arising in the gaming context are solved operationally by communicating with the customers via Skype, email, chat, or phone. The records of disputes are stored in the system.

7. RATIFICATION

The Policy will be valid for a period up to its annual or required reviewing.

This Policy has been duly executed this day of 29 January 2024.

Director eMagnus Curacao B.V.



1/29/2025

Andrea Engelhardt



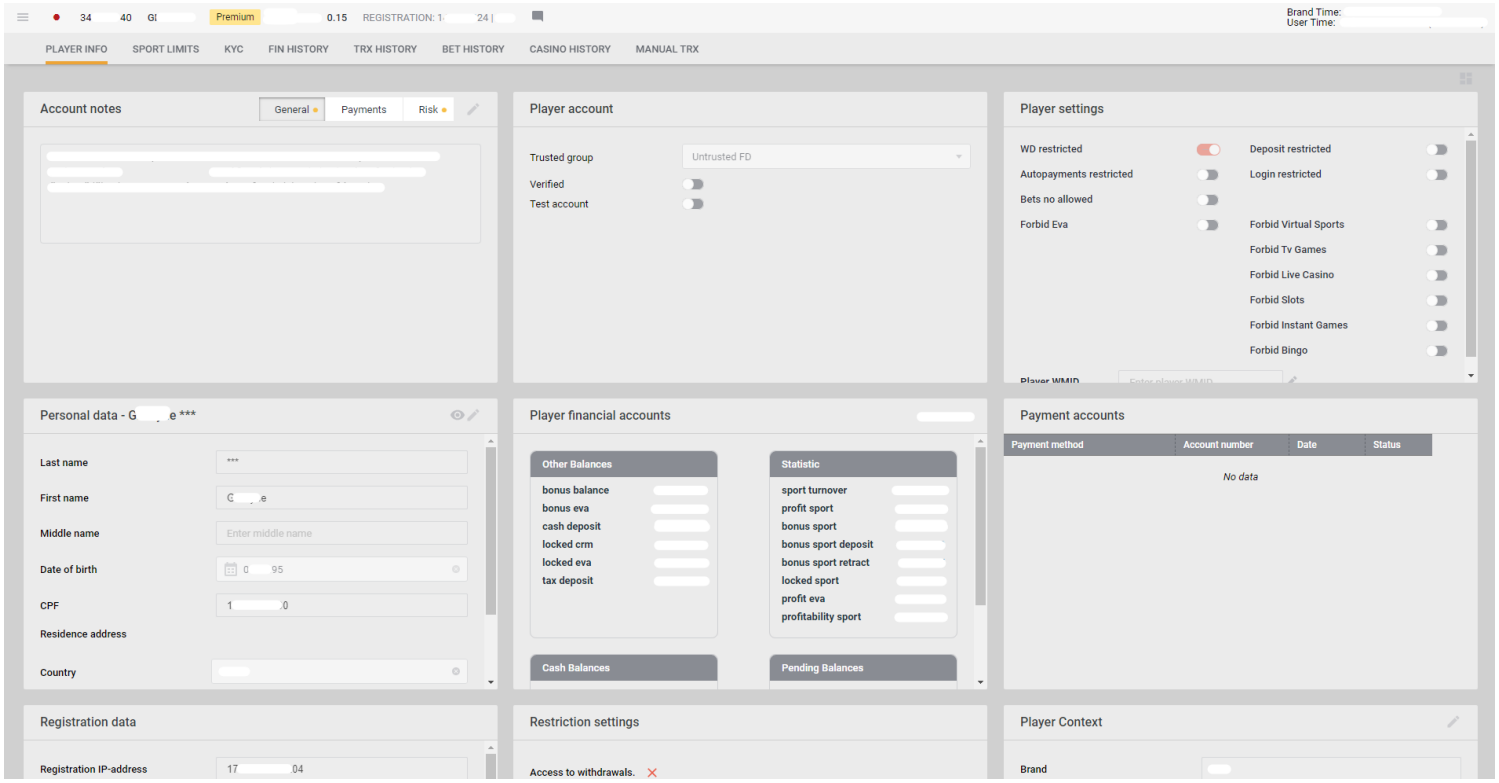
APPENDICES

APPENDIX A. OPERATING CONTROL MATRIX (FRAGMENT)

Number	Subareas	Control	Control type (prevention/detection)	Procedures description	When/ how often is performed/ trigger
1	Customers acceptance	Host country is monitored (prohibited: USA, Israel, France, Estonia, UK and outlying territories, Italy, Spain, Denmark, the Netherlands, Mohawk Territory of Kahnawae. list updates periodically)	prevention	System doesn't allow registration of the players from the prohibited countries	100% coverage
2	Customers acceptance	Age of the players is monitored	prevention	System doesn't allow registration of the players under 18 years	100% coverage
3	Customers acceptance	PEPs identification (KYC procedure)	detection	all the players are checked within PEPs list	100% coverage
4	Customers acceptance (1st deposit stage)	Only 1 account is allowed for 1 player	prevention	Table of first deposits is daily reviewed within the system - IP addresses are checked through "Search IP" button in the programme - deposits done through 1 wallet	100% coverage
5	Customers acceptance (1st deposit stage)	Full verification for risky players and full verification of the players where the country requires it (Belorussia)	prevention	Additional checks are performed for risky players: - passport copies - photo+passport copies - password sending to the registered address	Special criteria (risk country, risk currency, risk amount)
6	Customers acceptance (1st deposit stage)	Black-lists	prevention	all the players are automatically checked within the Black-lists in each Payment system	100% coverage
7	Customers acceptance (1st deposit stage)	PEP-lists check by PSPs	detection	all the players are automatically checked within the PEP-lists in each Payment system	100% coverage
8	Activation of account	Activation of the player can be done only after his e-mail check (it should be real)	prevention	Automatically generated link is sent to the registered e-mail of the player. The account will not be activated, till the link is followed	100% coverage

Responsible department	Who is doing?	To whom is reported?	Reports, back-ups, further actions
Automatic control	Automatic control	Automatic control	Account is not opened
Automatic control	Automatic control	Automatic control	Account is not opened
Automatic control	Automatic control	Head of Anti-fraud Departı	Restrictions to the account undertaken, request for additional documents sent to the player
Factoring and monitoring department	4-5 persons depending on the playing activity	The account is either blocked or agreed with the Head of the Department for blocking	Operational control, history of each player with comments can be reviewed in the system.
Factoring and monitoring department	4-5 persons depending on the playing activity	Operational review is done by the Head of the Department	Operational control, history of each player can be reviewed in the system
Automatic control	Automatic control	Automatic control	Account is blocked, notification sent to the player
Automatic control	Automatic control	Head of Payments Depart	Restrictions to the account undertaken, request for additional documents sent to the player
Automatic control	Automatic control	Automatic control	Automatic control

APPENDIX B. SAMPLE OF CUSTOMER TRACK-RECORD



APPENDIX C. REPORT ON SUSPICIOUS ACTIVITIES AND TRANSACTIONS

Date	Reporting officer	Description of suspicious activity or transaction	Area[3]	Mitigation measures taken NO / YES – description	Comments
…	…	…	…	…	…
…	…	…	…	…	…
…	…	…	…	…	…

[3] Customers / Deposits / Withdrawals / Betting rules / Revenue / ML&TF